Galois Theory

Issa Dababneh, School of Arts & Sciences, University of Bridgeport
Ryan McCulloch, School of Arts & Sciences, University of Bridgeport

Abstract

The proof of the unsolvability of quintic polynomials is usually attributed to Everiste Galois. However, Niels Abel first proved the unsolvability of quintics by drawing from the work of many earlier mathematicians such as Ruffini, Lagrange, Vandermonde, and Newton. Abel's impossibility proof is very convoluted and involves the nesting of radicals. Galois' approach is more elegant. Even though the general quintic is unsolvable, there exists quintics that are solvable. The power of Galois theory is its ability to discern which quintics are solvable. We explored modern Galois Theory through the classical lens of solving polynomial equations.

Galois Theory is the branch of mathematics which investigates the correspondence between the fields formed by the successive adjunction to a field F of the roots of a given polynomial equation, and the groups consisting of certain permutations on the set of these roots. The theory itself should be distinguished from its historically principal application which is the determination of necessary conditions for the solvability of equations by algebraic operations.

Generic Polynomials

If $t_1, \dots, t_n$ are independent variables, the polynomial

$$g(x) = \prod_{i=1}^{n} (x - \alpha_i)$$

is referred to as a generic polynomial. Since the roots, t_i, are independent, $g(x)$ is the most "general" polynomial of degree n and what we learn about $g(x)$ applies to all polynomials.

It can be shown that the generic polynomial can be written in the form

$$g(x) = x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n$$

where the coefficients are given by

$$s_1 = \sum_i \alpha_i \,, s_2 = \sum_{i<j} \alpha_i \alpha_j \,, s_3 = \sum_{i<j<k} \alpha_i \alpha_j \alpha_k \,, \dots$$

These are the elementary symmetric polynomials.

Newton's Theorem

A polynomial $p(\alpha_1, \dots, \alpha_n)$ in the variables $\alpha_1, \dots, \alpha_n$ is symmetric if it remains unchanged when we permute the variables. Each elementary symmetric polynomial is a symmetric polynomial of the roots. It follows that any polynomial in the coefficients of $g(x)$ is a symmetric polynomial of the roots .

Isaac Newton realized that a kind of converse to this holds: Any symmetric polynomial in the roots of $p(x)$ is a polynomial in the coefficients of $p(x)$.

1- A polynomial $p(\alpha_1, \dots, \alpha_n)$ is symmetric if and only if it is a polynomial in the elementary symmetric functions $s_1, \dots, s_n$ that is,

$$p(\alpha_1, \dots, \alpha_n) = q(s_1, \dots, s_n)$$

Moreover, if $p(t_1, \dots, t_n)$ has integer coefficients, then so does $q(s_1, \dots, s_n)$.

2- The set of symmetric polynomials in the roots of a polynomial $p(x)$ is the same as the set of polynomials in the coefficients of $p(x)$. In particular, any symmetric polynomial in the roots of $p(x)$ belongs to the same field as the coefficients, so if $p(x)$ is a polynomial over $\mathbb{Q}$, then any symmetric polynomial in the roots of $p(x)$ belongs to $\mathbb{Q}$.

When trying to find the roots of a polynomial , we can assume that any symmetric polynomial in the roots is known! An algorithm is known for computing the symmetric polynomials of the roots which requires knowing the coefficients of the polynomial only.

Lagrange Resolvents

Quadratic

$$u = (\alpha_1 + \alpha_2) = -b, \qquad v = (\alpha_1 - \alpha_2)$$

Cubic

$$v = {}^1\!/_3\,(\alpha_1 + \omega\alpha_2 + \omega^2\alpha_3), \qquad u = {}^1\!/_3\,(\alpha_1 + \omega^2\alpha_2 + \omega\alpha_3)$$

Quartic

$$u = {}^1\!/_2\,(\alpha_1 + \alpha_2 - \alpha_3 - \alpha_4), \qquad v = {}^1\!/_2\,(\alpha_1 - \alpha_2 + \alpha_3 - \alpha_4)$$
$$w = {}^1\!/_2\,(\alpha_1 - \alpha_2 - \alpha_3 + \alpha_4)$$

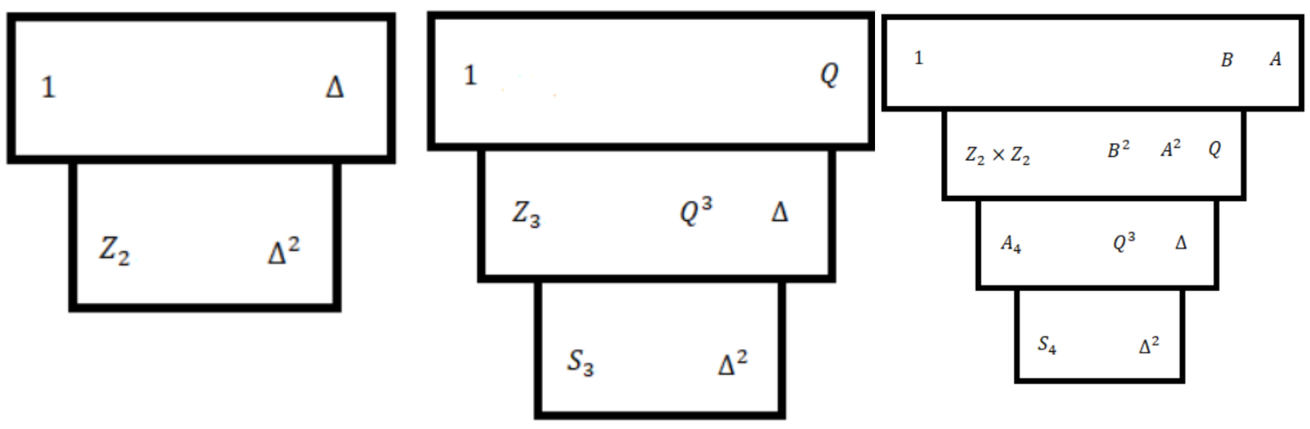
In the quadratic case, $\{v^2\}$ is closed under the permutation of roots. In the cubic case, $\{u^3, v^3\}$ is closed under the permutation of roots. In the quartic case, $\{u^2, v^2, w^2\}$ is closed under the permutation of roots.

$\alpha_1 + \alpha_2 = u$ and $\alpha_1 - \alpha_2 = v$, and u and v^2, using Newton's Theorem, can be computed.

$x^2 - (u^3 + v^3)x + u^3\, v^3 = 0$, and $u^3 + v^3$ and $u^3\, v^3$, using Newton's Theorem, can be computed.

$x^3 - (u^2 + v^2 + w^2)x^2 + (u^2v^2 + u^2w^2 + v^2w^2)x - u^2v^2w^2 = 0$, and $u^2 + v^2 + w^2$, $u^2v^2 + u^2w^2 + v^2w^2$, and $u^2v^2w^2$, using Newton's Theorem, can be computed.

Galois' Insight



In the case of the quadratic, $(\alpha_1 - \alpha_2)^2$ or Δ^2 is completely symmetric with respect to any permutation of the roots, Z_2.

In the case of the cubic, $(\alpha_1 + \omega\alpha_2 + \omega^2\alpha_3)^3$ and $(\alpha_1 + \omega^2\alpha_2 + \omega\alpha_3)^3$ are symmetric under Z_3 permutation of the roots. Then Δ^2 is symmetric under all permutations of the roots, S_3.

In the case of the quartic, $(\alpha_1 + \alpha_2 - \alpha_3 - \alpha_4)^2$, $(\alpha_1 - \alpha_2 + \alpha_3 - \alpha_4)^2$ and $(\alpha_1 - \alpha_2 - \alpha_3 + \alpha_4)^2$ are symmetric with to the $Z_2 \times Z_2$ permutation of the roots. Q^3 is symmetric with respect to the A_4 permutation of the roots. And Δ^2 is symmetric with respect to the Z_2 permutation of the roots.

According to Galois, if we can solve a general degree n polynomial by radicals, then we should be able to find a sequence of intermediate variables which satisfy lower degree polynomials.

Such intermediate variables should be fixed by subgroups of S_n. This is the crucial discovery of Galois that establishes the connection between groups and polynomials.

References

Roman, Steven. (2011). Field Theory (Graduate Texts in Mathematics) 2nd Edition. *World Publishing Company*, p.117.